




Ejercicio Práctico

 **Título:** Análisis y Propuesta de Mitigación y Prevención ante Múltiples Incidentes Simulados

Objetivo:

Evaluar la capacidad del estudiante para identificar medidas de mitigación y prevención adecuadas ante distintos tipos de incidentes, clasificarlos correctamente y diseñar una respuesta priorizada en función del riesgo y el impacto.

Escenario:




En la empresa ficticia **SecureWeb Ltd.**, el equipo de monitoreo detectó en las últimas 48 horas los siguientes eventos de seguridad:

1. **Múltiples intentos fallidos de login** desde la misma IP en un corto período de tiempo.
 2. **Inyección de código JavaScript** en los campos de comentarios del blog, que se ejecuta al ser visualizado por otros usuarios.
 3. Acceso no autorizado al endpoint `/admin/export` sin validación de rol.
 4. Uso de una librería JavaScript con **una vulnerabilidad conocida** no parcheada desde hace 3 meses.
 5. Fallo en el backend que **expone mensajes de error con estructura de base de datos** al público.
-

Actividades:

Parte 1 – Clasificación

1. Clasifica los cinco eventos entre:

-  **Incidente que requiere Mitigación inmediata**
-  **Riesgo prevenible por medidas previas (Prevención)**
-  **Ambos: requiere mitigar y prevenir**

Parte 2 – Propuesta técnica

2. Por cada evento, propone al menos **una medida de mitigación y una de prevención** específica (puede incluir código o herramienta si lo deseas).

Parte 3 – Prioridad de acción

3. Ordena los 5 eventos según su **riesgo e impacto inmediato**, justificando tu orden de prioridad para intervenir.

Entregables esperados:

- Tabla de clasificación por tipo de respuesta (mitigación / prevención / ambos).
- Propuesta técnica por evento con ejemplos claros.
- Lista priorizada de intervención con justificación basada en:
 - Nivel de exposición
 - Facilidad de explotación
 - Impacto sobre usuarios y datos

Recomendaciones:

- Puedes usar herramientas como WAF, SAST, CSP, análisis de logs, roles y políticas RBAC, actualizaciones de dependencias, validación de entradas, manejo de errores, etc.
- Justifica con fundamentos de buenas prácticas y principios del desarrollo seguro.